HAL
open science

A cryptoparty at the library, why, for whom and how

Damien Belvèze

To cite this version:

Damien Belvèze. A cryptoparty at the library, why, for whom and how. Bobcatsss 2016, Jan 2016, Lyon, France. , 2016. hal-01266276

HAL Id: hal-01266276

https://hal.science/hal-01266276v1

Submitted on 8 Apr 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

A CRYPTO PARTY At the Library

WHY, FOR WHOM, AND HOW?

WHO SOULD COME?

Students

> INSA students involved in privacy challenges (app building, embedded software designing)

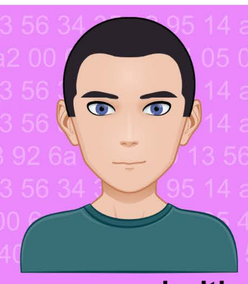
> other students (e.g : journalism, politics)

Librarians

> provide secured (?) wifi connexions to users

> Sign contracts with 3rd part vendors including user data

> should know a bit more about how DRM managers leak out personal data

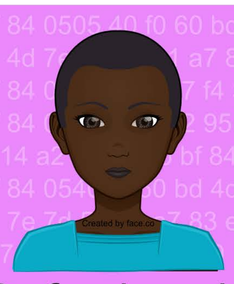


Concerned citizens

"And we are all involved" (Pascal)

> want to have control over their own data

> Are usually aware of mass surveillance and tracking by GAFAM



Professionnals

Could be for instance :

> Journalists trying to protect themselves and their sources

> Webmasters,

> Researchers esp. on sensitive matters

> policemen. And why not ?

WHO PERFORMS?

Teachers

> teach cryptography

> promote the event among their students

> organize the event with librarians

> manage workshops

Students

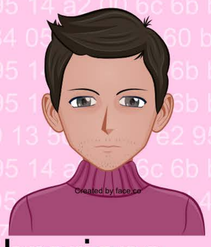
> study cryptography

> or use Tor or VPN for personal issues

Guest expert

> is in charge of the conference

> Could be a prof, senior officer, journalist specialized in security or electronic freedom challenges



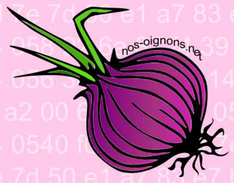
Librarians

> fight against auto-censorship due to mass surveillance

> try to protect user personal data

> Follow US activists from "Library Freedom project"

> would like to do the same in France. And why not ?



(h)ac(k)tivistes

> train attendees to privacy tools

> recruit new partners among students

> love onions

WORKSHOPS & TOOLKITS

Mail encryption

SSL Secure Connection

Data encryption, Integrity, Authentication

Anonymity network

Secure password management

WHY AT THE LIBRARY?

I have nothing to hide...

Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say (E. Snowden)

See the point, but I don't have enough time...

https everywhere takes only 15 secs to set up

IFLA Stated (14th August 2015)

"Data protection and privacy protection should be included as a part of the media and information literacy training for library and information service users. This should include training on tools to use to protect their privacy

Library and information services should reject electronic surveillance"

[Sharing Values | Improving Library System]

> Train users to secure communication and browsing

> Care about user data treatments by cloud service providers

> Display Tor on public PCs

> Build a Tor exit node for the library

There 's so much to be done...

CC:by-nc-sa damien.belveze@insa-rennes.fr

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES